CLAIMS

1. A method for enforcing a plurality of different policies on a stream of packets, the method comprising:

receiving a packet;

determining whether the packet corresponds to a common condition for a first policy rule and a second policy rule, the first policy rule belonging to a first policy type and the second policy rule belonging to a second policy type that differs from the first policy type; and

providing an association between the first packet and the common condition where it is determined that the packet corresponds to the common condition.

2. The method of claim 1, further comprising:

appending an extension to the packet and updating at least a first bit location in the extension to provide the association between the packet and the common condition.

3. The method of claim 1, further comprising:

determining whether the packet corresponds to a first particular condition for the first policy rule as compared to the second policy rule; and

determining applicability of the first policy rule to the packet where it is determined that

the common condition and the first particular condition correspond to the packet.

4. The method of claim 3, further comprising:

appending an extension to the packet;

updating at least a first bit location in the extension to provide the association between the packet and the common condition; and

updating at least a second bit location in the extension to provide the association between the packet and the first particular condition.

5. The method of claim 3, wherein determining applicability of the first policy rule to the packet comprises:

traversing a rule tree corresponding to the first policy rule, the rule tree having a first path corresponding to the first rule, the first path including the common condition and the first particular condition, wherein presence of the common condition and the first particular condition prompts a determination that the first policy rule is applicable to the packet.

6. The method of claim 1, wherein the first policy type is a firewall policy and the second policy type is a quality of service policy.

7. The method of claim 1, wherein the first and second policy types are selected from the following policy types: firewall, quality of service, intrusion detection.

8. The method of claim 1, further comprising:

creating a session for a plurality of session related packets including the packet; and

determining whether the packet corresponds to the common condition as evidenced from the created session.

9. The method of claim 8, further comprising:

updating at least a first bit location in an extension for each of the plurality of session related packets to associate each of the plurality of session related packets to the common condition.

10. The method of claim 3, further comprising:

creating a session for a plurality of session related packets including the packet; and

determining whether the packet corresponds to the first particular condition as evidenced from the created session.

11. The method of claim 10, further comprising:

updating at least a first bit location in an extension for each of the plurality of session related packets to associate each of the plurality of session related packets to the first particular condition.

12. The method of claim 3, further comprising:

determining whether the packet corresponds to a second particular condition for the second policy rule as compared to the first policy rule; and

determining applicability of the second policy rule to the packet where it is determined that the common condition and the second particular condition correspond to the packet.

13. The method of claim 12, wherein determining applicability of the first policy rule and the second policy rule to the packet comprises:

traversing a rule tree corresponding to the first policy rule and the second policy rule, the rule tree having a first path corresponding to the first rule and a second path corresponding to the second rule, the first path including the common condition and the first particular condition, the second path including the common condition and the second particular condition, wherein presence of the common condition and the first particular condition prompts a determination that the first policy rule is applicable to the packet, and presence of the common condition and the second particular condition prompts a determination that the second policy rule is applicable to the packet.

14. An apparatus for enforcing a plurality of different policies on a stream of packets, the apparatus comprising:

means for receiving a packet;

means for determining whether the packet corresponds to a common condition for a first

policy rule and a second policy rule, the first policy rule belonging to a first policy type and the second policy rule belonging to a second policy type that differs from the first policy type; and

means for providing an association between the first packet and the common condition where it is determined that the packet corresponds to the common condition.

15. The apparatus of claim 14, further comprising:

means for appending an extension to the packet and updating at least a first bit location in the extension to provide the association between the packet and the common condition.

16. The apparatus of claim 14, further comprising:

means for determining whether the packet corresponds to a first particular condition for the first policy rule as compared to the second policy rule, determining applicability of the first policy rule to the packet where it is determined that the common condition and the first particular condition correspond to the packet.

17. The apparatus of claim 16, further comprising:

means for appending an extension to the packet, updating at least a first bit location in the extension to provide the association between the packet and the common condition, and updating at least a second bit location in the extension to provide the association between the packet and the first particular condition.

18. The apparatus of claim 16, wherein determining applicability of the first policy rule to the packet comprises traversing a rule tree corresponding to the first policy rule, the rule tree having a first path corresponding to the first rule, the first path including the common condition and the first particular condition, wherein presence of the common condition and the first particular condition prompts a determination that the first policy rule is applicable to the packet.

19. The apparatus of claim 14, wherein the first policy type is a firewall policy and the second policy type is a quality of service policy.

20. The apparatus of claim 14, wherein the first and second policy types are selected from the following policy types: firewall, quality of service, intrusion detection.

21. The apparatus of claim 14, further comprising:

means for creating a session for a plurality of session related packets including the packet, and determining whether the packet corresponds to the common condition as evidenced from the created session.

22. The apparatus of claim 21, wherein the means for creating a session updates at least a first bit location in an extension for each of the plurality of session related packets to associate each of the plurality of session related packets to the common condition.

23. The apparatus of claim 16, further comprising:

means for creating a session for a plurality of session related packets including the packet, and determining whether the packet corresponds to the first particular condition as evidenced from the created session.

24. The apparatus of claim 23, wherein the means for creating a session updates at least a first bit location in an extension for each of the plurality of session related packets to associate each of the plurality of session related packets to the first particular condition.

25. The apparatus of claim 16, further comprising:

means for determining whether the packet corresponds to a second particular condition for the second policy rule as compared to the first policy rule, and determining applicability of the second policy rule to the packet where it is determined that the common condition and the second particular condition correspond to the packet.

26. The apparatus of claim 25, wherein determining applicability of the first policy rule and the second policy rule to the packet comprises traversing a rule tree corresponding to the first policy rule and the second policy rule, the rule tree having a first path corresponding to the first rule and a second path corresponding to the second rule, the first path including the common condition and the first particular condition, the second path including the common condition and the second particular condition, wherein presence of the common condition and the first

particular condition prompts a determination that the first policy rule is applicable to the packet, and presence of the common condition and the second particular condition prompts a determination that the second policy rule is applicable to the packet.

27. An apparatus for enforcing a plurality of different policies on a stream of packets, the apparatus comprising:

an infrastructure packet processing module group, which receives a packet; determines whether the packet corresponds to a common condition for a first policy rule and a second policy rule, the first policy rule belonging to a first policy type and the second policy rule belonging to a second policy type that differs from the first policy type, and provides an association between the first packet and the common condition where it is determined that the packet corresponds to the common condition.

28. The apparatus of claim 27, wherein the infrastructure packet processing module group appends an extension to the packet and updating at least a first bit location in the extension to provide the association between the packet and the common condition.

29. The apparatus of claim 27, further comprising:

a first policy processing module, in communication with the infrastructure packet processing module group, which determines whether the packet corresponds to a first particular condition for the first policy rule as compared to the second policy

rule, and determines applicability of the first policy rule to the packet where it is determined that the common condition and the first particular condition correspond to the packet.

30. The apparatus of claim 29, wherein the infrastructure packet processing module group appends an extension to the packet, updates at least a first bit location in the extension to provide the association between the packet and the common condition, and updates at least a second bit location in the extension to provide the association between the packet and the first particular condition.

31. The apparatus of claim 29, wherein determining applicability of the first policy rule to the packet comprises traversing a rule tree corresponding to the first policy rule, the rule tree having a first path corresponding to the first rule, the first path including the common condition and the first particular condition, wherein presence of the common condition and the first particular condition prompts a determination that the first policy rule is applicable to the packet.

32. The apparatus of claim 27, wherein the first policy type is a firewall policy and the second policy type is a quality of service policy.

33. The apparatus of claim 27, wherein the first and second policy types are selected from the following policy types: firewall, quality of service, intrusion detection.

34. The apparatus of claim 27, wherein the infrastructure packet processing policy module group comprises:

a session manager, which creates a session for a plurality of session related packets including the packet, and determines whether the packet corresponds to the common condition as evidenced from the created session.

35. The apparatus of claim 34, wherein the session manager updates at least a first bit location in an extension for each of the plurality of session related packets to associate each of the plurality of session related packets to the common condition.

36. The apparatus of claim 29, wherein the infrastructure packet processing module group comprises:

a session manager, which creates a session for a plurality of session related packets including the packet, and determines whether the packet corresponds to the first particular condition as evidenced from the created session.

37. The apparatus of claim 36, wherein the session manager updates at least a first bit location in an extension for each of the plurality of session related packets to associate each of the plurality of session related packets to the first particular condition.

38. The apparatus of claim 29, wherein the infrastructure packet policy module group

determines whether the packet corresponds to a second particular condition for the second policy rule as compared to the first policy rule, and determines applicability of the second policy rule to the packet where it is determined that the common condition and the second particular condition correspond to the packet.

39. The apparatus of claim 38, wherein determining applicability of the first policy rule and the second policy rule to the packet comprises traversing a rule tree corresponding to the first policy rule and the second policy rule, the rule tree having a first path corresponding to the first rule and a second path corresponding to the second rule, the first path including the common condition and the first particular condition, the second path including the common condition and the second particular condition, wherein presence of the common condition and the first particular condition prompts a determination that the first policy rule is applicable to the packet, and presence of the common condition and the second particular condition prompts a determination that the second policy rule is applicable to the packet.